

00463552

PCT/IL 98 / 00342



STATE OF ISRAEL

REC'D	19 AUG 1998
WIPO	PCT

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי
רצופים בזה העתקים
נכונים של המסמכים
שהופקדו לכתחילה
עם הבקשה לפטנט
לפי הפרטים הרשומים
בעמוד הראשון של
הנספח.

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

This 29-07-1998 היום

רשם הפטנטים
Registrar of Patents

נתאשר
Certified

לשימוש הלשכה
For Office Use

121389	מספר: Number
24-07-1997	תאריך: Date
הוקדם/נדחה Ante/Post-dated	

חוק הפטנטים, תשכ"ז - 1967
PATENT LAW, 5727 - 1967

בקשה לפטנט
Application for Patent

אני, (שם המבקש, מענו ולגבי גוף מאוגד - מקום התאגדותו)
(Name and address of applicant, and in case of body corporate-place of incorporation)

GraphiTech Ltd.
25 Herzl Street
Bnei-Braq 51364

גרפיטק בע"מ
רחוב הרצל 25
בני-ברק 51364

הדין _____ the Law
בעל אמצאה מכח _____
of an invention the title of which is _____ Owner, by virtue of

מערכת ושיטה לאימות חתימות

(בעברית)
(Hebrew)

SYSTEM AND METHOD FOR AUTHENTICATING SIGNATURES

(באנגלית)
(English)

hereby apply for a patent to be granted to me in respect thereof.

מבקש בואת כי ינתן לי עליה פטנט

• בקשת חלוקה - Application of Division		• בקשת פטנט מוסף - Application for Patent Addition		• דרישה דין קדימה Priority Claim	
מבקשת פטנט from Application	מס' No.	לבקשה/לפטנט to Patent/Appl.	מס' No.	מדינת האגוד Convention Country	תאריך Date
No. dated		No. dated			
הוגש בענין P.O.A.: general/individual- to be filed later- filed in case		הוגש בענין P.O.A.: general/individual- to be filed later- filed in case			
הען למסירת פטנטים בישראל Address for Service in Israel		הען למסירת פטנטים בישראל Address for Service in Israel			
662/97		662/97			
SELIGSOHN & GABRIEL		SELIGSOHN & GABRIEL			
ADVOCATES		ADVOCATES			
P.O.B. 1426, TEL-AVIV 61013		P.O.B. 1426, TEL-AVIV 61013			
חתימת המבקש Signature of Applicant		חתימת המבקש Signature of Applicant		היום 23 בחודש יולי שנת 1997 This of of the year	
				לשימוש הלשכה For Office Use	

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם בספר ובתאריך ההגשה, הנו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application the particulars of which are set out above.

Delete whatever is inapplicable מחק את המיותר

מערכת ושיטה לאימות חתימות

SYSTEM AND METHOD FOR AUTHENTICATING SIGNATURES

FIELD OF THE INVENTION

The present invention relates to a system and method for authenticating signatures in general and, in particular, to a
5 system and method for authenticating signatures transmitted over digital communication lines.

BACKGROUND OF THE INVENTION

10 In the field of computer graphics, it is known to use a digitizer to convert graphical data into electronic data for a computer. A user draws with an electronic pen on the digitizer tablet, and the digitizer converts the graphical data to electric signals. Such digitizers are used today for inputting data to computers, similar to a mouse.

15 There are many occasions in which it is necessary to authenticate the signature of a person signing a document in order to ensure that the signatory is indeed the person whose name is being signed. One particular application is the field of credit cards, wherein sums of money change hands in
20 reliance on the signature of the card holder. In the event that a card is stolen, a person who can forge the cardholder's signature can charge items against the cardholder's bank account. Similarly, when purchases are made over the telephone, the number and expiration date of the
25 card are read to the vendor, but there is no way to verify whether the caller is an authorized user of the card.

This problem has reached new heights with the advent of the Internet, where sales are transacted by means of transmitting the number and expiration date of the credit
30 card only, without any means of verifying the origin of the purchase. Since these communication lines are open, it is easy for a hacker to determine the number and expiration date of someone else's credit card which were transmitted over his modem, and to use that credit card for unauthorized
35 purchases.

Authentication of signatures by means of a graphical image (or bitmap) is not a solution because a photocopy of the signature looks authentic and cannot be detected.

Accordingly, there is a long felt need for and it would
5 be very desirable to have a method of authenticating the signature of a person, particularly a person using a credit card, both in a conventional sales transaction in a store, and over transmission lines, such as the Internet.

10 SUMMARY OF THE INVENTION

According to the present invention, there is provided a system for authenticating a signature including a digitizer, an electronic pen, a dynamic identification unit for measuring vectors produced during signature by the electronic
15 pen on the digitizer, and a comparator for comparing the vectors produced during signature with a reference signature.

According to a preferred embodiment, the system also includes an encryptor for encrypting a signature record and a decoder for decoding the encrypted signature record.

20 In accordance with the present invention, there is also provided a method of authenticating a signature including the steps of

providing a reference signature record,
signing with an electronic pen on a digitizer tablet,
25 calculating parameters from data produced during signing on the digitizer tablet;

comparing the parameters produced during signature with a reference signature record; and

30 providing an accept or reject response in accordance with results of the comparison.

According to a preferred embodiment, the method also includes the steps of encrypting the calculated parameters with a encryption key, and decrypting the encrypted data before comparing the parameters.

35 Further according to a preferred embodiment, the method includes the step of transmitting the calculated parameters

over a transmission line to a remote location before the step of comparing.

BRIEF DESCRIPTION OF THE DRAWINGS

5 The present invention will be further understood and appreciated from the following detailed description taken in conjunction with the drawings in which:

10 Fig. 1 is a schematic illustration of a signature authentication system according to one embodiment of the present invention;

 Fig. 2 is a flow chart of a method of providing a reference signature according to the invention;

 Fig. 3 is a flow chart of a method of authenticating a signature; and

15 Fig. 4 is a detail of a method of comparing the signature in the method of Fig. 3.

DETAILED DESCRIPTION OF THE INVENTION

20 The present invention relates to a system and method for authenticating signatures, the system and method being suitable also for authenticating signatures transmitted over communication lines. The present invention uses signature vector recognition and is based on the use of a digitizer together with software in a dynamic identification unit which
25 calculates parameters based on data produced during signature by the electronic pen on the digitizer tablet. These parameters, which are unique to each person when he signs his own name, are compared with the parameters in reference signature record, which is based on data produced during a
30 number of signatures, to determine whether the signature is authentic (i.e., signature by the authorized signatory) or forged.

 For purposes of the present invention, a digitizer refers to any device which is converts a location on an X,Y
35 tablet, possibly with the angle of the pen and the pressure on the pen, to a numerical value, and an electronic pen is any device by which a person can write or sign on a digitizer

tablet such that his handwriting can be detected by the digitizer. It will be appreciated that the system can be used to authenticate the handwriting of any predetermined word or words for which a reference record is made. Since the most
5 common words used to identify a person are his signature, the present application refers to signatures, by way of example.

It will be appreciated that there are many instances when it is desirable to authenticate the signature of a signatory, both in legal and business matters. The invention
10 will be described hereinbelow with relation to credit cards, for which it is particularly suitable, by way of example only, but those skilled in the art will appreciate that it can also be applied in any other instance of signature verification where the system components can be made
15 available.

When transmitting the signature over transmission lines for acceptance, as by a bank or credit card company, additional security can be provided by encrypting the signature with a secret key, known only to the signatory and
20 the bank, which cannot be determined by downloading the data containing the signature signals from the transmission line.

Referring now to Fig. 1, there is shown a schematic illustration of a system for authenticating a signature constructed and operative in accordance with one embodiment
25 of the invention. The system includes a digitizer 10 with an associated electronic pen 12 coupled to a computer 14 having a modem (not shown) for transmitting data from computer 14 to a remote location 16, generally a bank or credit card company in the present example. Digitizer 10 can be any conventional
30 digitizer, such as a Wacom Digitizer, manufactured by Wacom Co. Ltd., Japan.

At remote location 16, the data is received by a dynamic identification unit 20 arranged to receive the data produced during signature by the electronic pen on the digitizer
35 tablet and calculate therefrom a table of parameters which constitutes a signature record. The result is provided to a comparator 22 which compares the signature to be

authenticated with a reference signature record stored in its memory 24. If the signature is within predefined tolerances of the reference signature, comparator 22 sends an accept signal to computer 14. If the signature is not within the predefined tolerances of the reference signature, comparator 22 sends a reject signal to computer 14.

Operation of the system of the invention is as follows. First, a reference signature record must be provided for the bank or credit card company or other body which must accept or reject the signature, as shown in Fig. 2. This is done at the time of opening an account or requesting a credit card. The user signs his name on a digitizer tablet coupled to the computer of the credit card company. The pen position over the tablet is recorded by the computer to produce vectors, and a mathematical analysis is performed to learn the following parameters at any given time during the signature process:

- pen position (X,Y coordinates) over the tablet;
- sequences of drawing: number of letters, relative position, and time to draw;
- acceleration and deceleration during signature;
- direction changes.

Optionally the computer can also calculate pen tilt relative to the tablet and pen pressure, if the digitizer used is capable of providing this data. The digitizer data of the signature are input 30 to the dynamic identification unit in the computer. The dynamic identification unit records 32 the parameters of the signature. The recorded parameters are arranged 34 in a table of parameters. This process is repeated 36 a predetermined number of times, for example between 5 and 10, so as to permit the dynamic identification unit to calculate the tolerances 38 associated with the variations in the individual's signature, which is never identical. Once the parameter table and tolerances have been determined, these are stored in the computer memory for later reference as the reference signature record.

A personal ID code is also recorded 39 together with the signature vector table. This personal ID code serves as an encryption key to provide additional security for signature data transmitted over transmission lines. This encryption key
5 can be any string selected by the user which is known only to him and the credit card company. While the password selected by the credit card company, which is used in cash machines, etc. in conventional credit card authentication systems, can be used as the encryption key, it is preferable to select a
10 key which does not appear on the card. One example of a suitable encryption key is the user's birthdate.

It is a particular feature of the invention that the dynamic identification unit will recognize a person's signature even if it is signed upside down (i.e., where the
15 cardholder is in front of a counter) or rotated to any other angle, where the signature is smaller or larger in size, or slightly different in details.

At the time of making a credit card purchase, the purchaser's signature is authenticated as follows, as shown
20 in Fig. 3. The customer signs with an electronic pen on a digitizer tablet in the store or on the digitizer tablet coupled to his home computer. The record of the signature is received 40 by the credit card company. The dynamic identification unit retrieves 42 the reference signature
25 record of the cardholder. It may also retrieve 44 the personal ID code of the cardholder from the company computer if the signature is encrypted with the personal ID code. Generally this is necessary when making purchases other than at point of sale. If the record of the signature was
30 encrypted (described in detail hereinbelow) the record is now decrypted 46. If no recognizable signature record is received 48, the signature is rejected.

If the decryption results in a recognizable signature record, or if the signature record was not encrypted, the
35 dynamic identification unit proceeds to identify the signature 50, as shown in detail in Fig. 4. The dynamic identification unit traces 52 the vector lines in the

signature record and fills a parameter table 54 with the various parameters. The parameter table of the signature record is compared 56 with the reference parameter table stored in the computer memory.

5 Parameters for comparison are selected, for example, from the characteristics listed above. Any or all may be selected for use by the programmer. For example, the comparator can determine whether there is a significant difference in time of writing the signature 58, which could
10 indicate copying rather than an authentic signature. It can determine whether there is a difference in the number of vectors 60, i.e., whether a letter has been added or omitted. It can look for a change in the angle of the pen 62. It can determine whether there is a change in the relative direction
15 of the signature 63. And it can determine whether there are differences in pressure during signing 64. If any of the examined parameters is significantly different, i.e., outside the range of tolerances 66 (Fig. 3), the signature will be rejected. If the signature record meets all the
20 characteristics of the reference signature record, the signature will be authenticated and accepted. An indication of acceptance is then sent to the point of purchase.

 When making transactions at the point of sale, generally the physical lines are sufficiently secure that no encryption
25 is required, although it can be used, if desired. However, for transactions over the Internet, encryption is recommended to prevent theft of the credit card details. In this case, the Web surfer will have his own digitizer tablet coupled to his computer. After typing in the credit card number, as in
30 conventional credit card purchases over the net, a signature authentication software driver will pop an input window to the cardholder's screen. The cardholder will type his personal ID code and then sign his name on the digitizer tablet. The vectors produced during signature on the
35 digitizer tablet are calculated and the software encrypts the signature data using the personal ID code as the encryption key, as known.

The encrypted signature record is sent to the vendor, which may be a site on the Internet. The vendor forwards the signature record, as is, to the credit card company for authentication of the signature. When the encrypted signature
5 record reaches the credit card company, it is authenticated as described above with reference to Figs. 3 and 4. When the reference signature data of the cardholder is retrieved, the encryption key is also retrieved, permitting the dynamic identification unit to decrypt the signature record and
10 compare it with the reference signature. In accordance with the results of the comparison, the credit card company will notify the vendor that the signature is accepted or rejected.

It will be appreciated that the invention is not limited to what has been described hereinabove merely by way of
15 example. Rather, the invention is limited solely by the claims which follow.

CLAIMS

1. A system for authenticating a signature comprising:
 - (a) a digitizer and associated electronic pen ;
 - (b) a dynamic identification unit for receiving data
5 from said digitizer produced during signature by said electronic pen on said digitizer and calculating signature parameters therefrom;
 - (c) a transmitter for transmitting said calculated signature parameters for authentication;
 - 10 (d) a receiver for receiving said transmitted signature parameters;
 - (e) a comparator for comparing said received parameters produced during signature with a reference signature record; and
 - 15 (f) apparatus for providing an accept or reject response in accordance with the output of said comparator.
2. The system according to claim 1, wherein:
 - (a) said system further includes an encryptor for
20 encrypting said measured parameters to provide an encrypted signature record; and
 - (b) said dynamic identification unit further includes a decoder for decoding said encrypted signature record.
- 25 3. The system according to claim 1 or 2 for authenticating a signature transmitted over a transmission line comprising:
 - (a) a vendor unit including:
 - (1) a digitizer and associated electronic pen; and
 - (b) a signature authorization unit coupled to said
30 vendor unit by the transmission line and including:
 - (1) a dynamic identification unit for receiving data from said digitizer produced during signature by said electronic pen on said digitizer and calculating signature parameters therefrom;
 - 35 (2) a comparator for comparing said parameters produced during signature with a reference signature record; and

(3) apparatus for providing an accept or reject response to said vendor unit in accordance with the output of said comparator.

5 4. The system according to claim 1 or 2 for authenticating a signature transmitted over communication transmission lines comprising:

(a) a cardholder unit including:

(1) a digitizer and associated an electronic pen;

10 (2) apparatus for transmitting the output of said digitizer over the communication transmission lines;

(b) a signature authorization unit including:

15 (1) a dynamic identification unit for receiving data from said digitizer produced during signature by said electronic pen on said digitizer and calculating signature parameters therefrom;

(2) a comparator for comparing said parameters produced during signature with a reference signature record; and

20 (3) apparatus for providing an accept or reject response in accordance with the output of said comparator; and

25 (c) a vendor unit coupled to said cardholder unit and to said signature authorization unit by the communication transmission lines and including a transceiver for receiving said output of said digitizer from said cardholder unit and transmitting it to said signature authorization unit; and for receiving said accept or reject response from said signature authorization unit.

30

5. A method of authenticating a signature including the steps of:

(a) providing a reference signature record;

35 (b) signing with an electronic pen on a digitizer tablet;

(c) calculating signature parameters from data received from said digitizer produced during signature by said electronic pen on said digitizer;

(d) comparing said parameters produced during signature with said reference signature record; and

(e) providing an accept or reject response in accordance with results of the comparison.

6. The method according to claim 5, and further including the steps of:

(a) encrypting said calculated parameters with a encryption key after said step of calculating; and

(b) decrypting said encrypted parameters before comparing said parameters.

7. The method according to claim 5, wherein said step of providing a reference signature record includes:

(a) writing the signature on said digitizer several times;

(b) calculating signature parameters for each signature;

(c) calculating tolerances from an average reference signature from said signature parameters; and

(d) storing said average reference signature with said tolerances as a reference signature record.

8. The system according to any of claims 1-4 and substantially as shown and described hereinabove with reference to any of the drawings.

9. The system according to any of claims 1-4 and substantially as illustrated in any of Figs. 1-4.

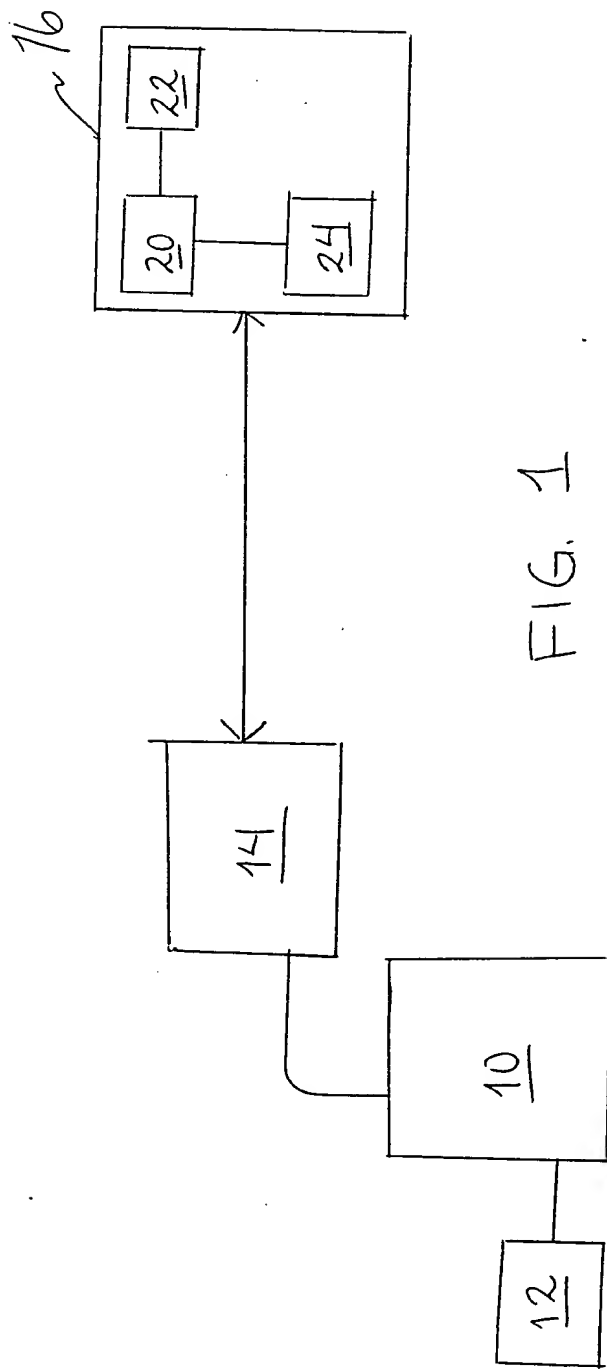
10. The method according to any of claims 5-7 and substantially as shown and described hereinabove with reference to any of the drawings.

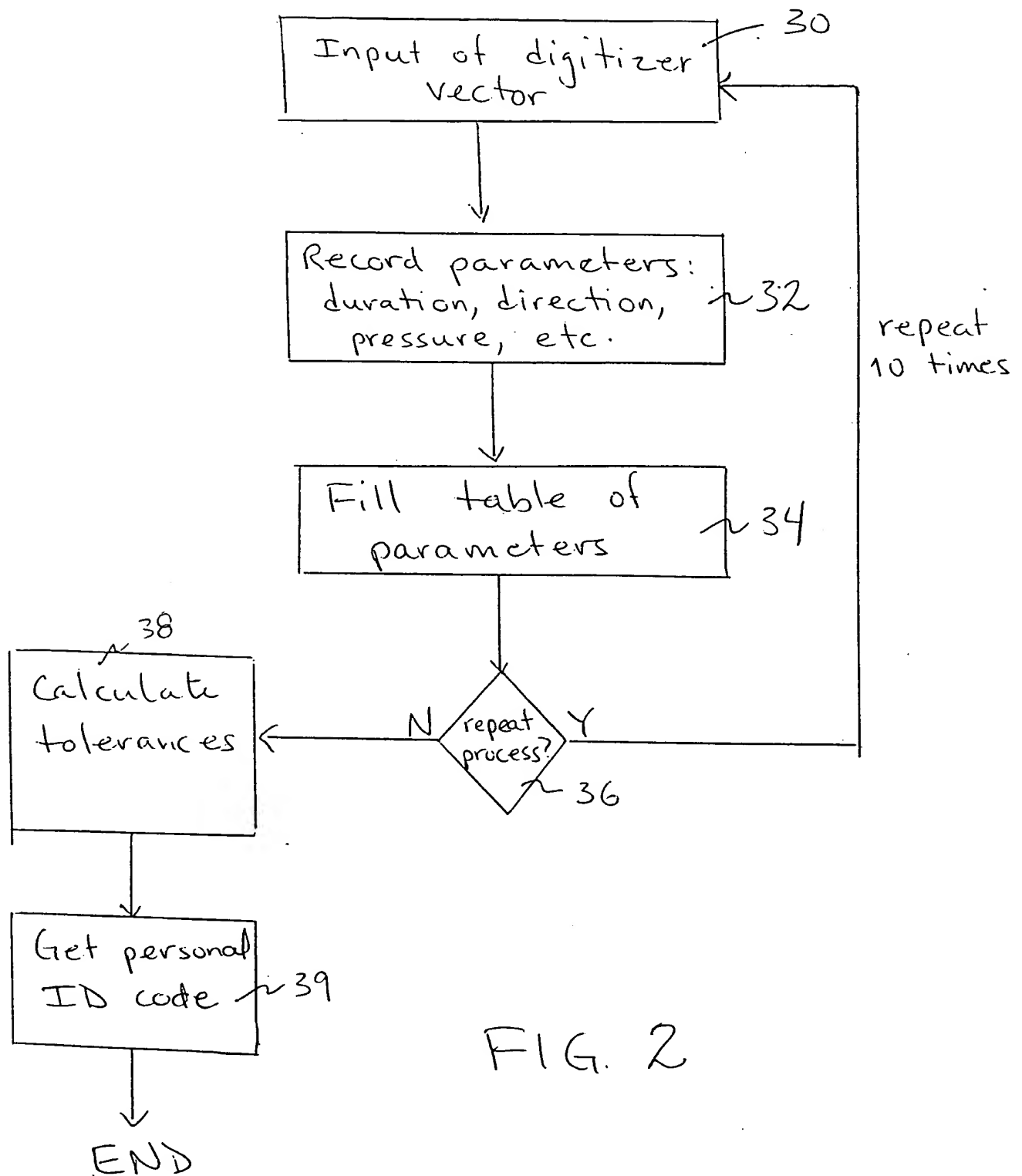
11. The system according to any of claims 5-7 and substantially as illustrated in any of Figs. 1-4.

5

De Gado

AGENT FOR APPLICANT
662-97ap.doc D-3





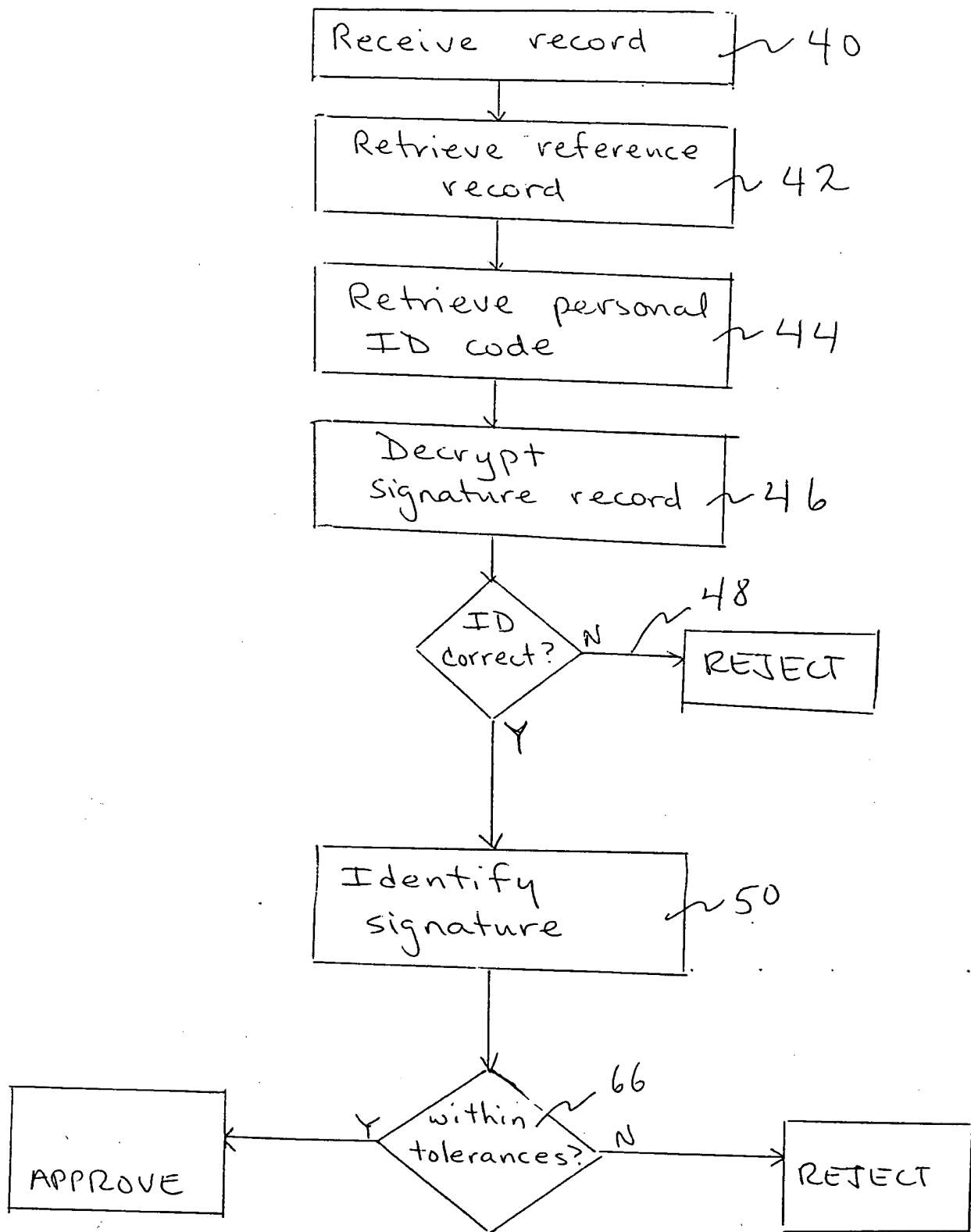


FIG. 3

